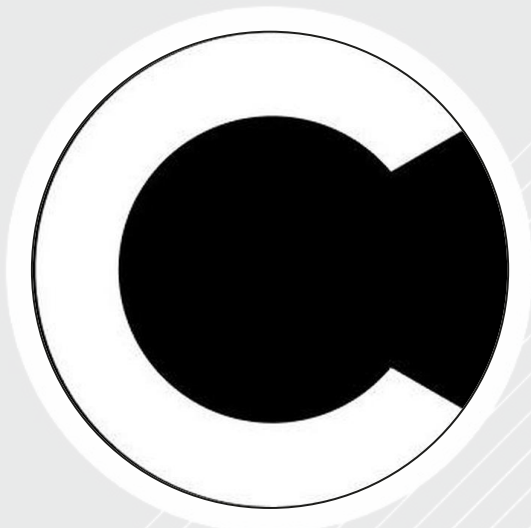




SPYWOLF

Security Audit Report



Completed on
June 15, 2023

@SPYWOLFNETWORK



@SPYWOLFNETWORK



SPYWOLF.CO





OVERVIEW

This audit has been prepared for **CAVEDAO** to review the main aspects of the project to help investors make an informative decision during their research process.

You will find a summarized review of the following key points:

- ✓ Contract's source code
- ✓ Owners' wallets
- ✓ Tokenomics
- ✓ Team transparency and goals
- ✓ Website's age, code, security and UX
- ✓ Whitepaper and roadmap
- ✓ Social media & online presence

“

The results of this audit are purely based on the team's evaluation and does not guarantee nor reflect the projects outcome and goal

- SPYWOLF Team -

”





TABLE OF CONTENTS

Project Description	01
Contract Information	02
Current Stats	03
Vulnerability Check	04
Threat Levels	05
Found Threats	06-A/06-B
Good Practices	07
Tokenomics	08
Team Information	09
Website Analysis	10
Social Media & Online Presence	11
About SPYWOLF	12
Disclaimer	13



CAVEDAO



PROJECT DESCRIPTION

According to their website:

With inspiration from the great philosopher Plato and his work “Allegory of The Cave”, the web3 space will experience things that never have been done before. Only if the true followers show their allegiance to the \$CAVE and It’s elemental powers.

People will be able to pledge their following to the \$CAVE by staking their mysterious \$CAVE tokens rewarding elemental attributes or pure aether as a reward.

Release Date: Presale starts in June, 2023

Category: Staking



CONTRACT INFO

Token Name
CAVE(DAO)

Symbol
CAVE

Contract Address

0x091f7f4c1db699a67d1342d6ac554e5d890db648

Network

Sepolia **TESTNET**

Language

Solidity

Deployment Date

Jun 14, 2023

Verified?

Yes

Total Supply

333,333

Status

Not launched

TAXES

Buy Tax
5%

Sell Tax
5%

*Taxes can be changed in future.



Our Contract Review Process

The contract review process pays special attention to the following:

- ✓ Testing the smart contracts against both common and uncommon vulnerabilities
- ✓ Assessing the codebase to ensure compliance with current best practices and industry standards.
- ✓ Ensuring contract logic meets the specifications and intentions of the client.
- ✓ Cross referencing contract structure and implementation against similar smart contracts produced by industry leaders.
- ✓ Thorough line-by-line manual review of the entire codebase by industry experts.

Blockchain security tools used:

- OpenZeppelin
- Mythril
- Solidity Compiler
- Hardhat



TOKEN TRANSFERS STATS

Transfer Count	TESTNET
Uniq Senders	TESTNET
Uniq Receivers	TESTNET
Total Amount	TESTNET
Median Transfer Amount	TESTNET
Average Transfer Amount	TESTNET
First transfer date	TESTNET
Last transfer date	TESTNET
Days token transferred	TESTNET

SMART CONTRACT STATS

Calls Count	TESTNET
External calls	TESTNET
Internal calls	TESTNET
Transactions count	TESTNET
Uniq Callers	TESTNET
Days contract called	TESTNET
Last transaction time	TESTNET
Created	TESTNET
Create TX	TESTNET
Creator	TESTNET



VULNERABILITY CHECK

Design Logic	Passed
Compiler warnings.	Passed
Private user data leaks	Passed
Timestamp dependence	Passed
Integer overflow and underflow	Passed
Race conditions and reentrancy. Cross-function race conditions	Passed
Possible delays in data delivery	Passed
Oracle calls	Passed
Front running	Passed
DoS with Revert	Passed
DoS with block gas limit	Passed
Methods execution permissions	Passed
Economy model	Passed
Impact of the exchange rate on the logic	Passed
Malicious Event log	Passed
Scoping and declarations	Passed
Uninitialized storage pointers	Passed
Arithmetic accuracy	Passed
Cross-function race conditions	Passed
Safe Zeppelin module	Passed
Fallback function security	Passed



THREAT LEVELS

When performing smart contract audits, our specialists look for known vulnerabilities as well as logical and access control issues within the code. The exploitation of these issues by malicious actors may cause serious financial damage to projects that failed to get an audit in time. We categorize these vulnerabilities by the following levels:

High Risk

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

Medium Risk

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

Low Risk

Issues on this level are minor details and warning that can remain unfixed.

Informational

Information level is to offer suggestions for improvement of efficacy or security for features with a risk free factor.



Informational

Owner can set buy/sell fees up to 10%.

Combined buy+sell = 20%.

When fees are above 0, there will be certain amount of tokens that will be deducted from every transaction that users make.

Deducted amount will be as much as the fees % from total amount that user had bought, sold and/or transferred.

```
function reduceFee(uint256 _feePercentage) external onlyOwner{
    require(_feePercentage <= 10 || _feePercentage < feePercentage);
    // 10% or less than before required
    feePercentage = _feePercentage;
    emit ConfigurationChange("feePercentage", _feePercentage);
}
```

Owner can exclude address from fees.

When address is excluded from fees, the user will receive the whole amount of the bought, sold and/or transferred tokens.

```
function setExcludeFromFee(address _address, bool _excluded) external onlyOwner {
    isExcludedFromFee[_address] = _excluded;
    emit ConfigurationChange("isExcludedFromFee", _excluded);
}
```



Informational

Owner can withdraw any tokens from the contract.

When this function is present, in cases tokens sent into the contract by mistake or purposefully, contract's owner can retrieve them.

```
function manualSendToken() external onlyOwner{
    IERC20(address(this)).transfer(msg.sender, balanceOf(address(this)));
}

function withdrawERC20(IERC20 token) external onlyOwner {
    uint256 balance = token.balanceOf(address(this));
    bool sent = token.transfer(msg.sender, balance);
    require(sent, "Failed to send token");
}

function withdrawETH() external onlyOwner {
    uint256 balance = address(this).balance;
    _sendViaCall(payable(msg.sender), balance);
}

function _sendViaCall(address payable _to, uint256 amountETH) internal {
    // Call returns a boolean value indicating success or failure.
    // This is the current recommended method to use.
    (bool sent, bytes memory data) = _to.call{value: amountETH}("");
    require(sent, "Failed to send Ether");
}
```



RECOMMENDATIONS FOR

GOOD PRACTICES

1

Consider fundamental tradeoffs

2

Be attentive to blockchain properties

3

Ensure careful rollouts

4

Keep contracts simple

5

Stay up to date and track development

CAVEDAO

GOOD PRACTICES FOUND

- ✓ The owner cannot mint new tokens after deployment
- ✓ The owner can set a transaction limit, but can't lower it than 1% of total supply
- ✓ The smart contract utilizes "SafeMath" to prevent overflows



There is no information about initial tokens distribution based on the project's whitepaper and/or website.

TOKENOMICS



THE TEAM

! The team is anonymous

KYC INFORMATION

! No KYC

We recommend the team to get a KYC in order to ensure trust and transparency within the community.





WEBSITE

Website URL

<https://www.cavedao.io/>

Domain Registry

<https://www.namecheap.com/>

Domain Expiration

2024-05-30

Technical SEO Test

Passed

Security Test

Passed. SSL certificate present

Design

Very nice design with appropriate color scheme and graphics.

Content

The information helps new investors understand what the product does right away. No grammar mistakes found..

Whitepaper

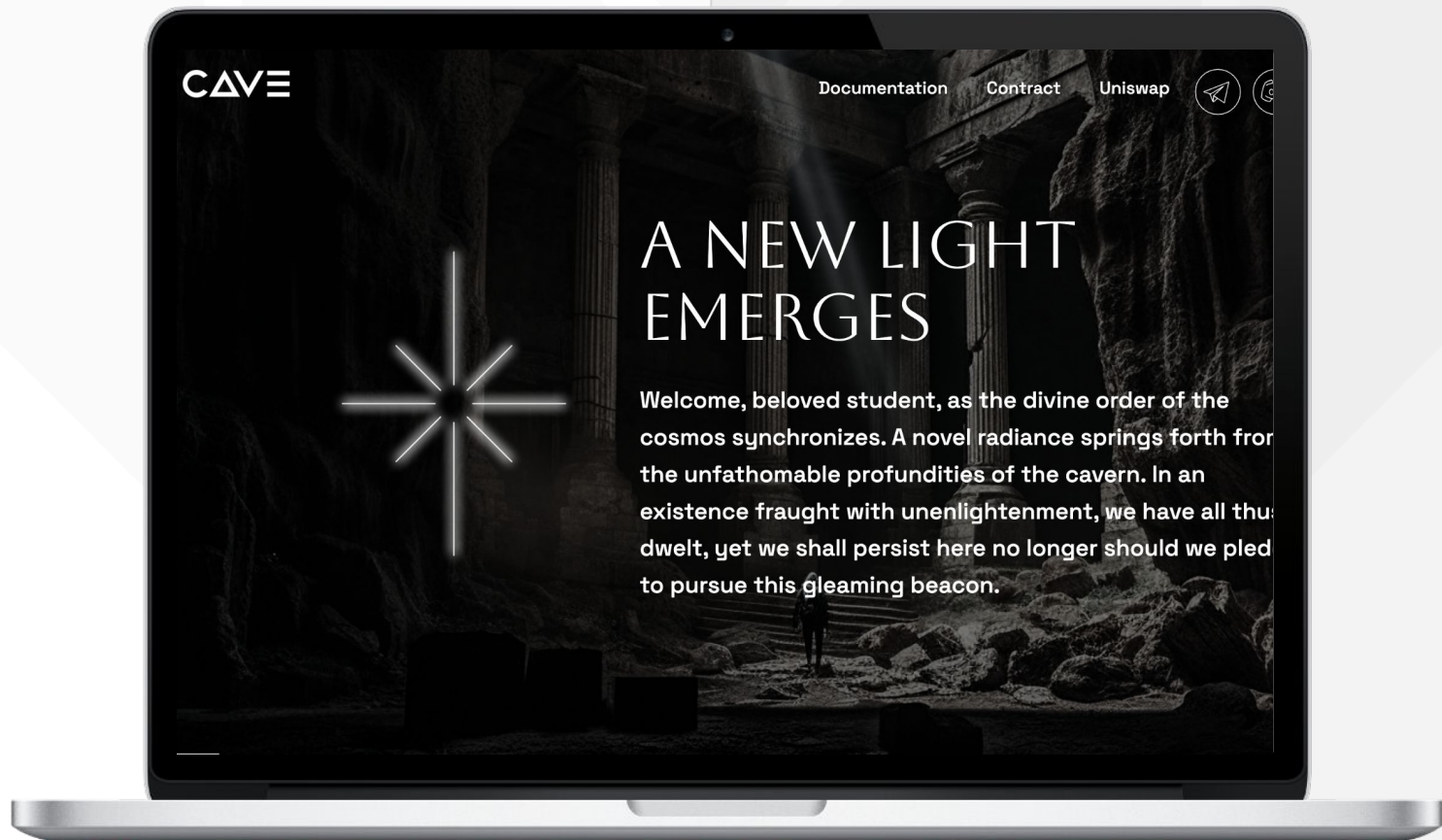
Yes, explanatory.

Roadmap

No

Mobile-friendly?

Yes



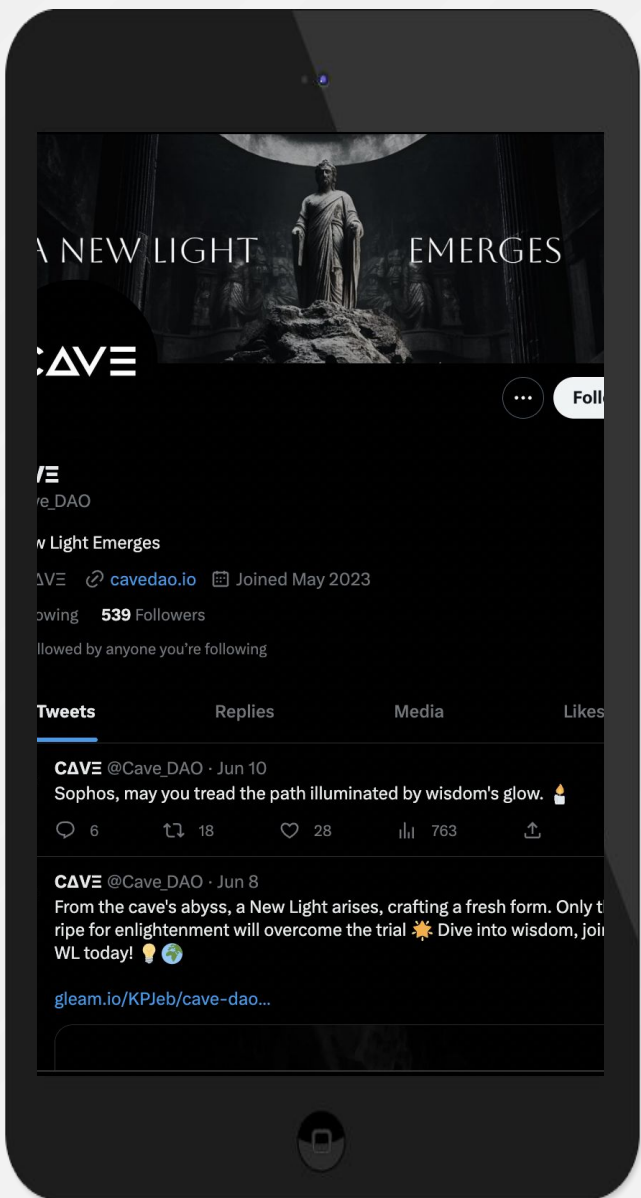
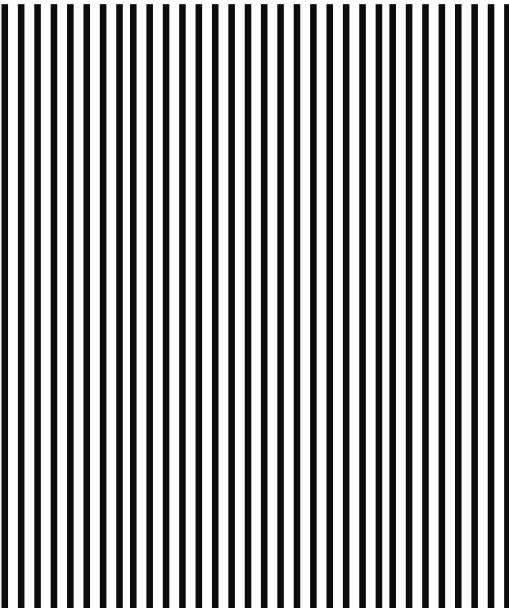
cavedao.io



SOCIAL MEDIA & ONLINE PRESENCE



ANALYSIS
Project's social media
pages are active



Twitter

@cave_dao

- 837 followers
- 4 total posts
- New account



Discord

<https://discord.com/invite/BZkq88cwBv>

- 546 members
- Active members
- Active mods



Telegram

@cavedaoportal

- 363 members
- Active members
- Active mods



Medium

- Not available



SPYWOLF

CRYPTO SECURITY

Audits | KYCs | dApps
Contract Development

ABOUT US

We are a growing crypto security agency offering audits, KYCs and consulting services for some of the top names in the crypto industry.

- ✓ OVER 500 SUCCESSFUL CLIENTS
- ✓ MORE THAN 500 SCAMS EXPOSED
- ✓ MILLIONS SAVED IN POTENTIAL FRAUD
- ✓ PARTNERSHIPS WITH TOP LAUNCHPADS, INFLUENCERS AND CRYPTO PROJECTS
- ✓ CONSTANTLY BUILDING TOOLS TO HELP INVESTORS DO BETTER RESEARCH

To hire us, reach out to
contact@spywolf.co or
t.me/joe_SpyWolf

FIND US ONLINE



[SPYWOLF.CO](https://spywolf.co)



[@SPYWOLFNETWORK](https://t.me/SPYWOLFNETWORK)



[@SPYWOLFNETWORK](https://twitter.com/SPYWOLFNETWORK)



Disclaimer

This report shows findings based on our limited project analysis, following good industry practice from the date of this report, in relation to cybersecurity vulnerabilities and issues in the framework and algorithms based on smart contracts, overall social media and website presence and team transparency details of which are set out in this report. In order to get a full view of our analysis, it is crucial for you to read the full report.

While we have done our best in conducting our analysis and producing this report, it is important to note that you should not rely on this report and cannot claim against us on the basis of what it says or doesn't say, or how we produced it, and it is important for you to conduct your own independent investigations before making any decisions. We go into more detail on this in the disclaimer below – please make sure to read it in full.

DISCLAIMER:

By reading this report or any part of it, you agree to the terms of this disclaimer. If you do not agree to the terms, then please immediately cease reading this report, and delete and destroy any and all copies of this report downloaded and/or printed by you. This report is provided for information purposes only and on a non-reliance basis, and does not constitute investment advice.

No one shall have any right to rely on the report or its contents, and SpyWolf and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers and other representatives) (SpyWolf) owe no duty of care towards you or any other person, nor does SpyWolf make any warranty or representation to any person on the accuracy or completeness of the report.

The report is provided "as is", without any conditions, warranties or other terms of any kind except as set out in this disclaimer, and SpyWolf hereby excludes all representations, warranties, conditions and other terms (including, without limitation, the warranties implied by law of satisfactory quality, fitness for purpose and the use of reasonable care and skill) which, but for this clause, might have effect in relation to the report. Except and only to the extent that it is prohibited by law, SpyWolf hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against SpyWolf, for any amount or kind of loss or damage that may result to you or any other person (including without limitation, any direct, indirect, special, punitive, consequential or pure economic loss or damages, or any loss of income, profits, goodwill, data, contracts, use of money, or business interruption, and whether in delict, tort (including without limitation negligence), contract, breach of statutory duty, misrepresentation (whether innocent or negligent) or otherwise under any claim of any nature whatsoever in any jurisdiction) in any way arising from or connected with this report and the use, inability to use or the results of use of this report, and any reliance on this report. The analysis of the security is purely based on the smart contracts, website, social media and team.

No applications were reviewed for security. No product code has been reviewed.